

Re: Environment Poisoning and login –p

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-02/0157.html>

From: Andrew McNaughton (andrew_at_scoop.co.nz)

Date: 02/28/04

Date: Sat, 28 Feb 2004 15:54:01 +1300 (NZDT)

To: freebsd-security@freebsd.org

On Fri, 27 Feb 2004, Peter Pentchev wrote:

> On Fri, Feb 27, 2004 at 05:13:53AM –0600, D J Hawkey Jr wrote:

> > On Feb 26, at 03:03 PM, Tim Kientzle wrote:

> > >

> > > Andrey Chernov wrote:

> > > > On Wed, Feb 25, 2004 at 10:54:31AM –0800, Tim Kientzle wrote:

> > > >

> > > > > Possible fix: Have login unconditionally discard LD_LIBRARY_PATH

> > > > > and LD_PRELOAD from the environment, even if "-p" is specified.

> > > >

> > > > Yes! It is what I say from very beginning. It is so obvious that I wonder

> > > > why others not see it first.

> > >

> > > Instead, I've decided to follow Jacques Vidrine's

> > > suggestion of using a whitelist of environment variables

> > > that are "known-safe."

Sounds sensible for me, but it exaggerates the need for a configuration file.

In the sudo man page under 'SECURITY NOTES', there's some details of a blacklist approach taken by sudo, dealing with similar issues. Worth looking at while considering the extent of this problem, and because omissions in sudo's blacklist are likely to have been discussed somewhere already.

> > Coming in from left field... Will there be some sort of mechanism for
> > an admin to set/modify this list?

> Surely you are aware of the consequences of s/admin/intruder/? :)

> Still, it might be useful indeed.

If the intruder already has root, there's not much to lose here.

Andrew McNaughton

--

Re: Environment Poisoning and login –p

FreeBSD-Security: Re: Environment Poisoning and login -p

No added Sugar. Not tested on animals. May contain traces of Nuts. If irritation occurs, discontinue use.

Andrew McNaughton Currently in Boomer Bay, Tasmania
andrew@scoop.co.nz
Mobile: +61 422 753 792 <http://staff.scoop.co.nz/andrew/cv.doc>

freebsd-security@freebsd.org mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-security>
To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"